The UK-US Data Bridge — advantages and challenges

Sharon Lamb, Partner, Pilar Arzuaga, Senior Associate and Michaela Novakova, Associate, with McDermott Will & Emery UK LLP, comment on the UK-US Data Bridge

The UK-US Data Bridge has been operational from 12th October 2023, enabling UK businesses to transfer personal data to US organisations that (i) are listed on the EU-US Data Privacy Framework (‘DPF’), and (ii) participate in the UK Extension to the DPF more easily. This initiative, falling under the UK Extension to the DPF, is governed by Article 45 of the UK General Data Protection Regulation (the ‘UK GDPR’). It streamlines the data transfer process to the US, bypassing the need for the additional safeguards that Articles 46 and 49 of the UK GDPR typically require.

The European Commission adopted its adequacy decision for the DPF on 10th July 2023. The decision concluded that the DPF ensures an adequate level of protection for transferring personal data from the EU to the US.

The DPF is a bespoke, opt-in certification scheme enforced and administered by various US departments which supersedes the earlier Privacy Shield. It sets out a series of mandatory principles and requirements that US organisations must certify and adhere to, significantly shaping how organisations handle, collect, and disclose personal data.

US organisations which are listed on the DPF and also participate in the UK-US Data Bridge are recognised as providing an adequate level of data protection from the transfers from the UK.

Historical context

The DPF and the UK-US Data Bridge are results of continuous evolution. Before the EU-US Privacy Shield, there was the Safe Harbor agreement, established in 2000. Safe Harbor was an arrangement that allowed for the transfer of personal data from the EU to the US, provided that US companies adhered to principles that were deemed to provide adequate protection.

However, concerns about US surveillance practices and the adequacy of the Safe Harbor agreement led to its invalidation by the European Court of Justice in 2015 in a landmark case, Schrems I (C-362/14). This ruling underscored the need for stronger safeguards and more stringent compliance mechanisms to protect the personal data of EU citizens when transferred across the Atlantic.

In response to the invalidation of Safe Harbor, the EU-US Privacy Shield was established in 2016. It was designed as a more robust legal mechanism to align with EU data protection rules for transatlantic data transfers. This framework introduced stronger obligations on US companies to protect the data of Europeans and provided for better monitoring and enforcement by US authorities.

However, the Privacy Shield also faced challenges and criticisms, particularly regarding US surveillance practices and the rights of EU citizens to access legal remedies. These concerns ultimately led to the invalidation of the Privacy Shield by the European Court of Justice in Schrems II (C-311/18) in 2020. This decision once again highlighted the need for a more resilient and comprehensive framework to govern transatlantic data transfers, paving the way for the development of the current DPF.

The landscape of data protection and transatlantic data transfers was further complicated by Brexit. The UK’s departure from the EU meant that it no longer fell under the EU’s data protection frameworks, necessitating the establishment of separate data transfer agreements. This led to the development of the UK-US Data Bridge, a tailored mechanism to ensure the continuation of seamless and secure data transfers between the UK and the US.

The EU Data Privacy Framework

The DPF aligns with UK GDPR principles, covering aspects like purpose limitation, data retention, data minimisation, security and accuracy. It addresses the deficiencies of the EU-US Privacy Shield, and introduces enhanced data protection measures, including restrictions on US intelli-
gence services’ access to EU personal data, ensuring it is both necessary and proportionate.

Further, the framework outlines a comprehensive redress procedure for EU individuals who have concerns. As a first step, EU individuals can approach their national Supervisory Authority with complaints that can be transmitted to the US for investigation and binding resolution by Civil Liberties Protection Officer. Should the resolution be unsatisfactory, individuals can appeal for a review by a newly established Data Protection Review Court.

Not all US organisations can participate in the DPF and by extension in the UK-US Data Bridge. Eligibility is confined to those under the jurisdiction of the US Federal Trade Commission or the Department of Transportation. This exclusion presents a notable limitation for sectors like banking, insurance, and telecommunications, which currently cannot participate in the DPF programme.

How does the Data Bridge mechanism work?

The UK-US Data Bridge allows certified US companies to receive personal data from the UK by extending the DPF.

The concept of a data bridge within the UK framework is an adequacy decision that enables the transfer of personal data from the UK to other countries without additional protective measures. Central to a data bridge is the adherence to UK GDPR regulations, ensuring the protection of personal data of UK individuals during international transfers.

Evaluating a data bridge encompasses reviewing the data protection practices, rule of law, human rights adherence, and regulator effectiveness of the recipient country. This mechanism is vital for maintaining the integrity of personal data protection under the UK GDPR when data are transferred internationally.

Suffice to say, the UK-US Data Bridge does not absolve UK businesses of their responsibilities under UK data protection laws. These responsibilities include safeguarding data, especially sensitive health information, and upholding the rights of data subjects. This ensures that data sent from the UK to accredited US organisations are protected robustly.

Advantages and challenges of using the DPF and the UK-US Data Bridge

The DPF provides organisations with a streamlined approach to data transfers. Organisations that participate in the DPF are automatically deemed safe for receiving personal data from the UK.

One of the prime benefits of the UK-US Data Bridge is that participating organisations are exempted from the need to conduct transfer impact assessments (‘TIA’s”) or institute supplementary measures. In contrast, if companies rely on Standard Contractual Clauses (‘SCCs’) or Binding Corporate Rules (‘BCRs’), they are still mandated to implement supplementary measures. The UK-US Data Bridge facilitates a seamless transfer of data back and forth between the two territories. Further, as the data protection landscape evolves, customers increasingly expect companies to actively participate in such data transfer framework, enhancing trust and compliance.

However, both the UK Information Commissioner’s Office (‘ICO’) and EU privacy activists have raised doubts about the UK-US Data Bridge and the DPF. The ICO noted in its opinion on the UK-US Data Bridge Regulations that there are areas that could pose risks to UK data subjects if the protections identified are not properly applied.

The opinion identifies several potential issues with the UK-US Data Bridge, which may serve as a basis to question its legitimacy. First, it does not contain substantially similar rights to the UK GDPR’s (i) right to be forgotten, (ii) right to withdraw consent, and (iii) right to obtain a review of an automated decision by a human. As a result, UK data subjects might not have the same level of control over their data as they do under the UK GDPR.

The definition of ‘sensitive information’ under the UK-US Data Bridge does not specify all the ‘special categories of personal data’ of the UK GDPR. Instead, the framework has a broad ‘umbrella’ concept providing that sensitive information can be any data regarded as sensitive by the transferring entity. UK businesses will have to clearly label certain types of data as ‘sensitive’ when transferring to a US organisation certified under the UK-US Data Bridge to ensure adequate protection.

For data on criminal offences, the ICO highlights potential vulnerabilities. Since the UK places restrictions on the use of ‘spent’ convictions, there are concerns about a lack of comparable protections in the US for transferred data.

EU privacy activists have already challenged the DPF before the Court of Justice of the European Union (‘CJEU’), advocating for its prompt suspension. However, the CJEU rejected this request, pointing to the applicant’s inability to show urgency and the risk of significant harm without the suspension. Still, we anticipate more developments on this front.

UK data protection activists have also voiced criticism, suggesting that the UK-US Data Bridge may not deliver on its promises to provide enforcea-
(Continued from page 11)

ble rights and effective remedies against any potential misuse of personal data.

Practical tips for UK organisations

UK organisations intending to use the UK-US Data Bridge should:

• verify the recipient’s certification with the DPF;
• confirm the recipient’s participation in the UK-US Data Bridge;
• review the recipient’s privacy policy for compliance, and if transferring human resources data, check that the policy provides information about such HR transfers;
• update their own privacy policies to reflect data transfers using the UK-US Data Bridge; and
• assess the categories of data being transferred, in particular ensuring special category data are correctly labeled as ‘sensitive’ to the US recipient.

Organisations should remember that if they cannot rely on the UK-US Data Bridge to transfer personal data to the US, they will have to revert to one of the pre-existing appropriate safeguards (e.g., the International Data Transfer Agreement or the UK Addendum to the EU Standard Contractual Clauses) or rely on one of the available derogations under Article 49 of the UK GDPR for international data transfers. Organisations may also need to carry out a transfer risk assessment to validate transfers using the pre-existing appropriate safeguards.

Conclusion

While the DPF and UK Data Bridge present advantages for organisations aiming for seamless data transfers from the EU or the UK to the US, they are not without challenges. It is advisable for eligible US organisations to consider the merits of self-certification.

The DPF and the UK-US Data Bridge extension are not the only option organisations have for transferring and processing personal data outside of the UK. Controllers or processors may still choose to rely on other appropriate safeguards such as SCCs or BCRs. With evolving regulations and growing customer expectations, US organisations might find certification increasingly important.

Given the changing landscape, we are witnessing a rising number of organisations diversifying their safeguard measures, anticipating potential changes or challenges to existing transfer mechanisms.

Sharon Lamb, Pilar Arzuaga and Michaela Novakova
McDermott Will & Emery UK LLP
slamb@mwe.com
parzuaga@mwe.com
mnovakova@mwe.com

(Continued from page 11)